



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/456,794	12/08/1999	JAY C. CHEN	34581/CAG/C718	6924

7590 12/31/2002

McDermott Will & Emery
Attn: Craig A. Gelfound
2049 Century Park East
34th FL
Los Angeles, CA 90067-3208

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 12/31/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/456,794

Applicant(s)

CHEN, JAY C.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 October 2002.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 54-116 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 54-116 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12-8-1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 15 October 2002 that cancelled claims 1-53, added claims 54-116, submitted drawings pointing out labels, and replaced the brief summary of the invention.

Drawings

2. The drawings are objected to because elements 1-10 in figure 2 and 50 and 1180 in figure 12 are not labeled. Correction is required. Numbers do not count as labels.

Response to Arguments

3. Applicant's arguments filed 15 October 2002 have been fully considered but they are not persuasive.

4. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., pre-loading public keys on smartcards) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2132

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 54, 55, 81 rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al. (6240091) in view of Schneier.

In lines 51-67 of column 7, Ginzboorg et al. present a smart card that includes, among other pieces of data, the public key of a second party. As evidenced by the abstract and billing system (BS) in figure 3a, Ginzboorg et al. complete a transaction. They do not teach the specific steps of the claims. In describing the Woo-Lam protocol described on page 64, Schneier shows, in step 3, Alice initiating communications with Bob by encrypting a message (Bob's name and a random challenge) with Bob's public key and sending it to him. Bob, by contacting Trent and decrypting the response generates a session key K. He then encrypts Trent's signature, which contains K, with Alice's public key, thereby formatting a key exchange response message, and sends it to her. Alice uses the session key to encrypt Bob's challenge (sent with Trent's signature), and the transaction is completed. Schneier's method provides authentication and a symmetric key. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the teachings of Schneier in Ginzboorg et al.'s system so as to both authenticate parties and in order to provide the parties with a symmetric key. As such the limitations of claims 54, 55, 81 are met.

7. Claims 56-74 and 82-102 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al. in view of Schneier as applied to claims 54, 55, and 81 above, and further in view of Walker et al. (6263438).

Ginzboorg et al. and Schneier teach a smart card that contains a second entity's public key. The smart card and second entity authenticate themselves to one another and agree on a symmetric key. There is no teaching of sending the smart card's public key to the second entity. In lines 38-52 of column 6, Walker et al. teach including digital certificates (which include encrypted forms of an originator's public key) with messages to provide greater assurance. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send a certificate with Alice's first message, as taught by Walker et al., to provide greater assurance.

As this applies to the claims, 56 is clearly rendered obvious. Step 5 in the Woo-Lam protocol involves the second entity providing a challenge, meeting additional limitations of claim 57. Schneier teaches signing messages on pages 576 and 577. Ginzboorg et al. also teach signatures in, for example, their abstract. This renders obvious signing all messages sent from one entity to another. 58 is obvious because of this teaching and the additional payment steps shown by Ginzboorg et al.

Ginzboorg et al., Schneier, and Walker et al. do not mention using the symmetric key to protect information, such as account information, a transaction amount, and sensitive transaction data. Official notice is taken that it is old and well known for a purchaser to encrypt data, including account information, a transaction amount, and sensitive transaction data, with a symmetric key in an electronic transaction in order to prevent that data from being used illicitly. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt transaction data sent between the two entities in order to protect data. Data that need

not be protected should not be, thereby reducing cryptographic operations and meeting the limitations of claims 60 and 62.

Ginzboorg et al., Schneier, and Walker et al. has not mandated that the entities include transaction identifiers with their transaction correspondences. Official notice is taken that it is old and well known to include transaction identifiers assigned by one entity with their transaction correspondences, which helps catalog and identify messages. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include transaction identifiers with their transaction correspondences in order to track messages.

8. Claims 75-80 and 103-116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al., Schneier, and Walker et al. as applied to claim 54 above, and further in view of Thompson et al.

Ginzboorg et al., Schneier, and Walker et al. teach a method for exchanging keys. They do not show the group method of key request. Thompson et al show a method by which changes to a document are recorded. This method entails signing all changes. For the purposes of this discussion, we will assume that Thompson et al.'s original bill corresponds to applicant's key exchange request. As can be seen in figure 5, the original bill has been signed by the originator and then modified and signed by a second entity, whereby the original bill remains perceptible. The benefit of this is that it allows parties to know exactly what different entities added, as taught in lines 29 and 30 of column 5. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include signatures and recognizable updates

as taught by Thompson et al. in Schneier's key exchange requests, thereby piggybacking requests and reducing the total number of transmissions of data.

Different session keys would be the most obvious, as the requesting entities have made no indication of wanting to communicate with each other. However, a scenario where two requesting entities desired the same key so that they could communicate securely is also obvious.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703)

305-1338. The examiner can normally be reached on between 9 AM and 6 PM,
Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
December 18, 2002

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134